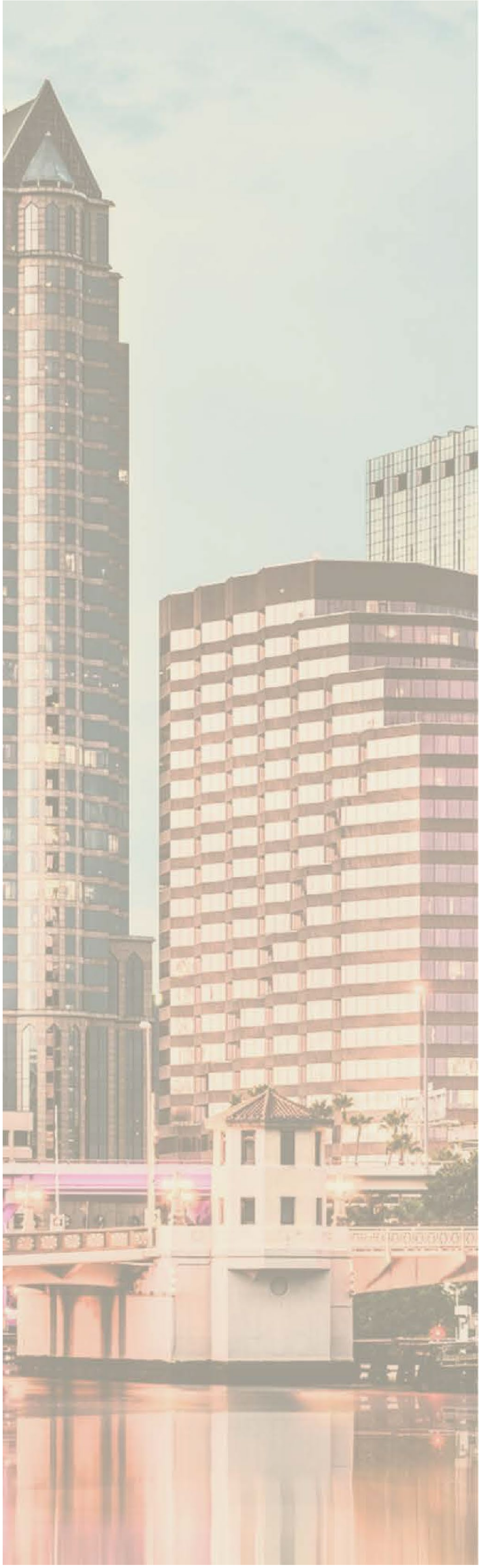


VICTOR D. CRIST

CLERK OF CIRCUIT COURT & COMPTROLLER
HILLSBOROUGH COUNTY, FL

EXCELLENCE IN SERVICE!

★ ★ ★ ★ ★

COUNTY AUDIT DEPARTMENT

REPORT # 432

MARCH 17, 2025

An Audit of:

IT ASSET INVENTORY CONTROLS

VICTOR D. CRIST

CLERK OF CIRCUIT COURT & COMPTROLLER
HILLSBOROUGH COUNTY, FL

The Honorable Ken Hagan, Chair
The Honorable Chris Boles
The Honorable Donna Cameron Cepeda
The Honorable Harry Cohen
The Honorable Christine Miller
The Honorable Gwen Myers
The Honorable Joshua Wostal

March 17, 2025

Dear Commissioners:

The Audit Team conducted an audit of the Information and Innovation Office (IIO) Asset Inventory Controls (**Audit Report #432, dated March 17, 2025**). Responses to the Audit Team's recommendations were received from the Director of the Information Technology Department and have been included in the Report after each audit comment and recommendation.

The purpose of this Report is to furnish management with an independent, objective analysis, and information concerning the activities reviewed. It is not an appraisal or rating of management.

Although the Audit Team exercised due professional care in the performance of this audit, this should not be construed to mean that unreported noncompliance or irregularities do not exist. The deterrence of fraud and/or employee abuse is the responsibility of management. Audit procedures alone, even when carried out with professional care, do not guarantee that fraud or abuse will be detected.

I appreciate this opportunity to be of service to the Board of County Commissioners. I am happy to address any questions that you may have or furnish additional information if desired.

Sincerely,

Heidi Pinner

Heidi Pinner, CIA CISA CFE CRMA
Chief Audit Executive, Clerk of Court & Comptroller

TABLE OF CONTENTS

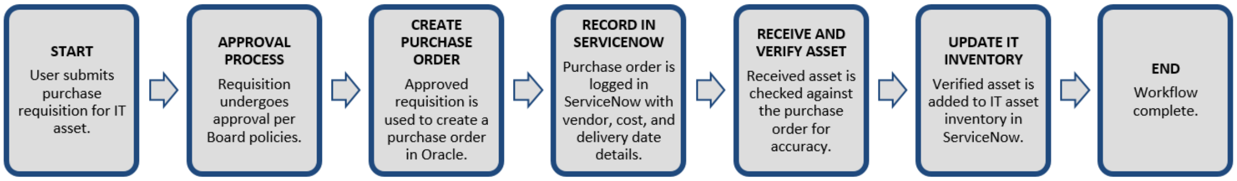
EXECUTIVE SUMMARY

BACKGROUND INFORMATION

IT asset management, also referred to as IT inventory management, is a business process encompassing financial, contractual, and inventory functions to support the life cycle management of IT assets. These assets can include all software and hardware that are found in the business environment. This audit focuses on the IT hardware assets managed by the Information Technology Department (ITD), which falls under the Board of County Commissioners (Board) Information & Innovation Office (IIO). These assets are managed using a web-based system called ServiceNow. Hardware asset management involves overseeing the physical components of computers and computer network components, from acquisition through disposal.

ServiceNow provides the Board with a unified, web-based platform for requesting, approving, and tracking IT assets throughout their life cycle, including procurement, management, redeployment, and disposal.

The system allows users across county departments to submit purchase requisitions for IT assets, which then undergo the following process:


START
User submits purchase requisition for IT asset.
APPROVAL PROCESS
Requisition undergoes approval per Board policies.
CREATE PURCHASE ORDER
Approved requisition is used to create a purchase order in Oracle.
RECORD IN SERVICENOW
Purchase order is logged in ServiceNow with vendor, cost, and delivery date details.
RECEIVE AND VERIFY ASSET
Received asset is checked against the purchase order for accuracy.
UPDATE IT INVENTORY
Verified asset is added to IT asset inventory in ServiceNow.
END
Workflow complete.

ServiceNow tracks key asset details, such as ownership, location, maintenance schedules, and service history. The platform also provides reporting capabilities, offering visibility into the IT asset inventory, including asset counts, values, and other relevant metrics.

OBJECTIVE

The objective of the audit is to determine whether or not adequate controls are in place for the management of the Board's technology-related assets managed by the ITD.

SCOPE

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*. These Standards require that County Audit plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit comments, and conclusions based on the audit objectives. County Audit believes that the evidence obtained provides this reasonable basis.

The audit scope covered the controls and processes related to IT hardware assets managed through the "ServiceNow" system as of August 2024. Audit procedures included interviews with key personnel, analysis of asset data, review of user access to ServiceNow, and IT asset sample testing of various county locations.

OVERALL EVALUATION

PROCESS STRENGTHS AND SUCCESSES

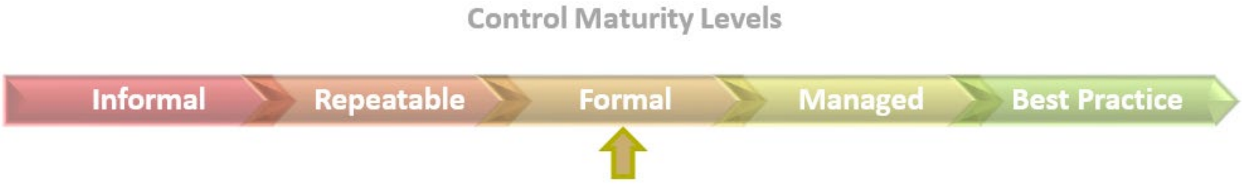
- **ServiceNow is properly utilized for requesting, approving, and recording of IT assets.**
- **Asset tagging procedures are being properly performed.**
- **Proper steps are taken to sanitize and decommission end-of-life IT assets.**
- **Capital assets are accurately documented and updated in Oracle.**
- **Decommissioned assets are appropriately recorded and transferred to Surplus.**

CONTROL IMPROVEMENT OPPORTUNITIES/RISKS

- **Lack of periodic user access review has resulted in terminated employees and unknown users retaining access in ServiceNow, increasing the risk of unauthorized access.**
- **Discrepancies in system records were identified across multiple locations.**

Full testing results are included in page 5 of this Report.

OPINION



The overall control environment relative to the management of the County's IT asset inventory is at a formal (defined) maturity level. This means that management has established controls to ensure IT assets are properly procured, tagged, and recorded in the ServiceNow system. Additionally, sanitization and decommissioning procedures are being effectively performed. Opportunities exist to enhance the user de-provisioning process and improve the update of IT locations and asset transfers after deployment in the ServiceNow system.

The exit conference was held with Hillsborough County's Information & Innovation Office on February 7, 2025.

Other minor concerns not included in this Report were communicated to management and/or corrected during fieldwork.

AUDITED BY

Heidi Pinner, CIA, CISA, CFE, CRMA, Chief Audit Executive
Raul Cardona, CIA, CISA, CSXA, IT Audit & Advisory Services Manager
Shane Sandie, Internal Auditor

AUDIT COMMENT 1: USER ACCESS CONTROLS

357 USER ACCOUNTS REVIEWED

68 EXCEPTIONS IDENTIFIED

45 ACCOUNTS USER'S STATUS COULD NOT BE DETERMINED

21 ACCOUNTS LINKED TO TERMINATED EMPLOYEES

PERIODIC USER ACCESS REVIEWS SHOULD BE PERFORMED

An opportunity exists to improve the de-provisioning process of user accounts in the ServiceNow system.

The objective was to determine whether or not ServiceNow accounts were assigned to authorized active internal or external users in line with their roles and responsibilities.

Background

The ServiceNow system simplifies and automates the IT assets management process by integrating with the County's active directory and employing role-based access controls. Based on these roles assigned, only authorized individuals should have the ability to access the system, place orders for computers, and other IT related equipment.

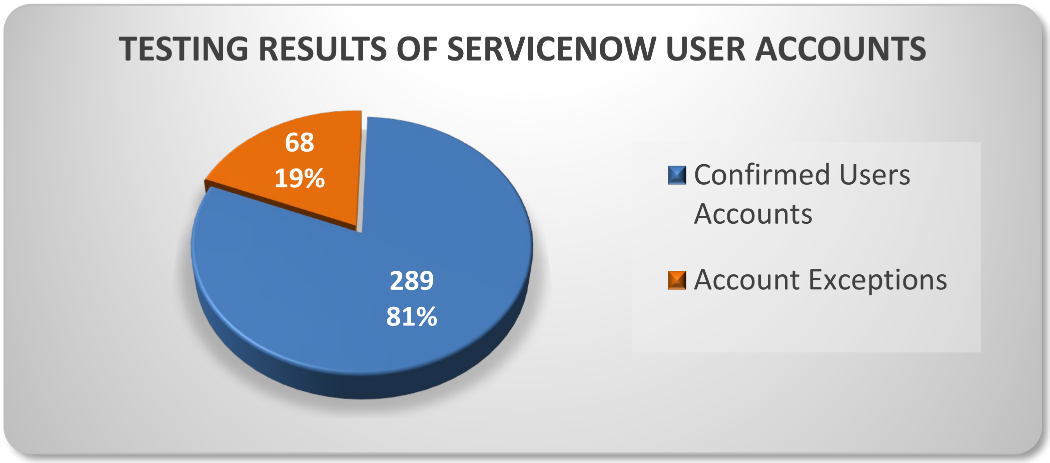
TEST PROCEDURE

The Audit Team performed the following steps:

1. Obtained a complete list of 357 ServiceNow user accounts.
2. Retrieved a recent list of active and terminated Hillsborough County employees.
3. Used data analytics to compare the list of user accounts against the lists of active and terminated employees.
4. Followed up with the ITD to research, clarify, and identify any discrepancies.
5. Documented any findings, including user accounts belonging to terminated employees, third-parties no longer working with the County, and unknown user accounts.

TESTING RESULTS

Out of 357 user accounts with access to ServiceNow, 68 user accounts (19%) were identified as exceptions.



These 68 identified exceptions included:

- Forty-five (45) user accounts which could not be matched to either active employees, terminated employees, or the County directory lists.
- Twenty-one (21) accounts for users identified on the terminated employee list.
- Two (2) user accounts for a single user (duplicate account).

RECOMMENDATION

Even when a system relies on Active Directory for authentication, security best practices recommends disabling user accounts at the application level to reduce the risk of unauthorized access.

Management should establish and document a periodic review of ServiceNow user accounts and their assigned configuration management database (CMDB) permissions to ensure that only authorized personnel have access. Additionally, third-party access should be proactively monitored, and former employees and external user accounts should be promptly disabled in the system to support compliance with system access policies.

CLIENT RESPONSE:

Concur

CORRECTIVE ACTION PLAN:

The Information Technology Department (ITD) has established and implemented a process to disable inactive user accounts at the application level. For third-party user accounts not managed in Oracle, the Server team processes deactivation requests via the Technology Service Portal, after which the user records are also inactivated in ServiceNow. Additional items included in the action plan:

- *ITD has implemented a process to disable user accounts at the application level through the Technology Service Portal for employees and third-party contractors.*

- *To enhance validation, the team will continue reviewing HR termination reports and verifying its accuracy in ServiceNow.*

- *Conduct monitoring of third-party user accounts and remind supervisors managing third-party contractors to submit Non-Employee Account Requests for contractor terminations.*

TARGET COMPLETION DATE:

June 30, 2025

AUDIT COMMENT 2: ACCURACY OF INVENTORY RECORDS

676
DEPLOYED ASSETS TESTED

383
IN-STOCK ASSETS TESTED

97%
DEPLOYED ASSETS CONFIRMED

100%
IN-STOCK ASSETS CONFIRMED

Reasonable controls are in place for the tracking and management of deployed IT assets.

The objective was to determine whether or not the IT Asset Inventory is accurate and complete by confirming asset records in ServiceNow. This included conducting physical verification of assets, assessing the alignment of asset data with procurement and movement documentation, and ensuring proper tagging in accordance with County policy.

Background

IT assets procured through ServiceNow are delivered to the ITD IT asset warehouse, where they are verified against purchase orders for accuracy in description, quantity, and cost. Assets are tagged based on their classification:

- Capital assets (>$4,999.99) receive white tags and the information is submitted to County Finance for proper recording in Oracle.
- Non-capital assets (<$5,000.00) are tagged with yellow labels and entered into the ServiceNow inventory system.

Applicable configuration tasks (e.g., imaging) are completed before assets are designated for deployment. The deployment process varies based on the equipment type. Assets not immediately needed are added to “in stock” inventory. For deployment-ready equipment, the Asset Management Department notifies the requestor via email, the requestor’s name is added to the package and prepared for pickup.

TEST PROCEDURE

Population, Sample Selection and IT Inventory Assets Testing

The Audit Team obtained a complete list of all Board IT assets tracked in ServiceNow as of January 2024 and analyzed the data to select County locations for testing. Locations with the highest volume of deployed and in-stock assets were prioritized.

Testing of Deployed Assets - “Floor to System” Approach

Based on the population analysis, the Audit Team judgmentally selected the following eight (8) County locations for testing between March and April 2024:

#	Hillsborough County Location	Asset Quantity
1	Brandon Safety Operations Complex (BSOC)	73
2	County Center (CC) 25th Floor	68
3	Head Start	73
4	John F. Germany Library	52
5	Lee Davis Center	31
6	Museum of Science and Industry (MOSI)	186
7	Public Safety Operations Complex (PSOC) Data Center	140
8	Public Utilities (PU) Administrative Building	53
	Total Assets Reviewed	**676**

At each location, the Audit Team utilized the "floor to system" approach, starting with a physical count of IT assets on-site and then comparing the counts to the corresponding data in ServiceNow. This method is effective for verifying that all physically present items are accurately reflected in the inventory system.

Testing of In-Stock Assets – “System to Floor” Approach

For in-stock assets, the Audit Team performed testing at the IT warehouse located in 419 N. Pierce St using a "system to floor" approach. This method begins with a review of asset records in ServiceNow, followed by verifying the physical location of the selected sample items in the warehouse. This approach is effective for validating the existence of items and confirming that their current physical locations match the inventory records in ServiceNow.

By employing both the "floor to system" and "system to floor" approaches, the Audit Team ensured a comprehensive evaluation of both deployed and in-stock IT assets.

TESTING RESULTS

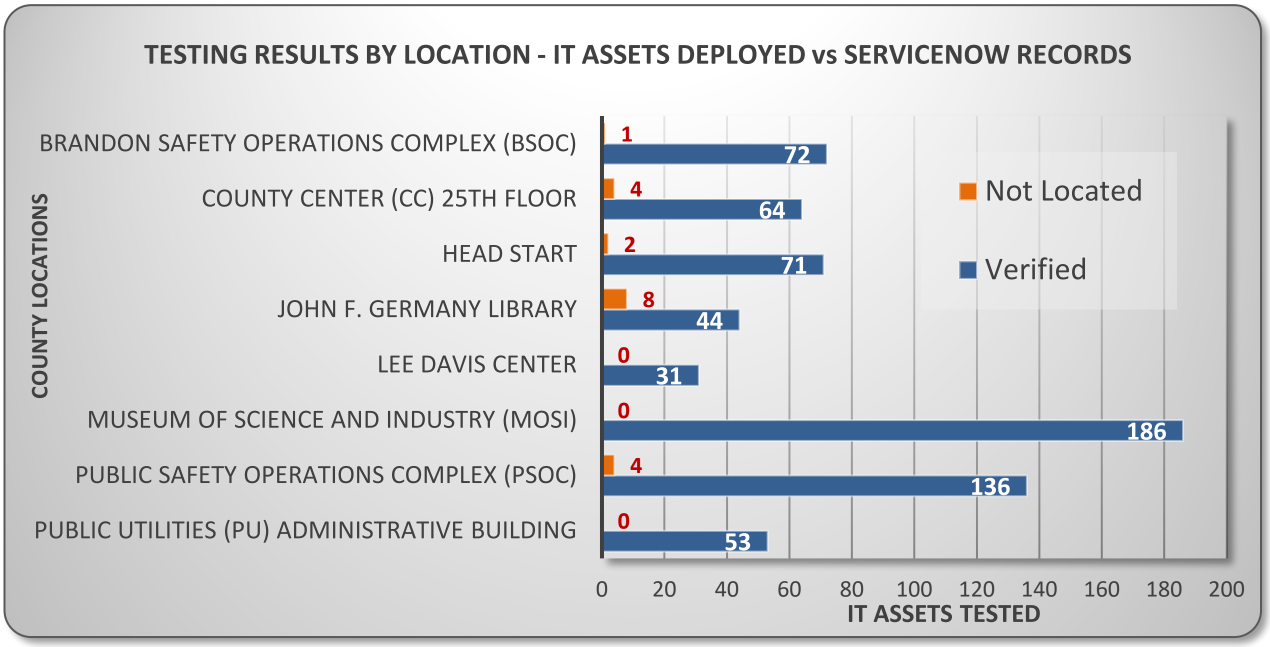
Observations from Sample Selection

The Audit Team utilized the ServiceNow data to select the locations for testing. Some locations in the ServiceNow data appeared to be outdated, such as the Net Park location, which showed 753 deployed IT assets. The IT Team was unable to provide an explanation for these records, stating that Net Park was used by the County several years ago. Per audit review, it appears that the data has not been updated to reflect the movement or disposal of these IT assets.

Testing of Deployed (In-use) Assets

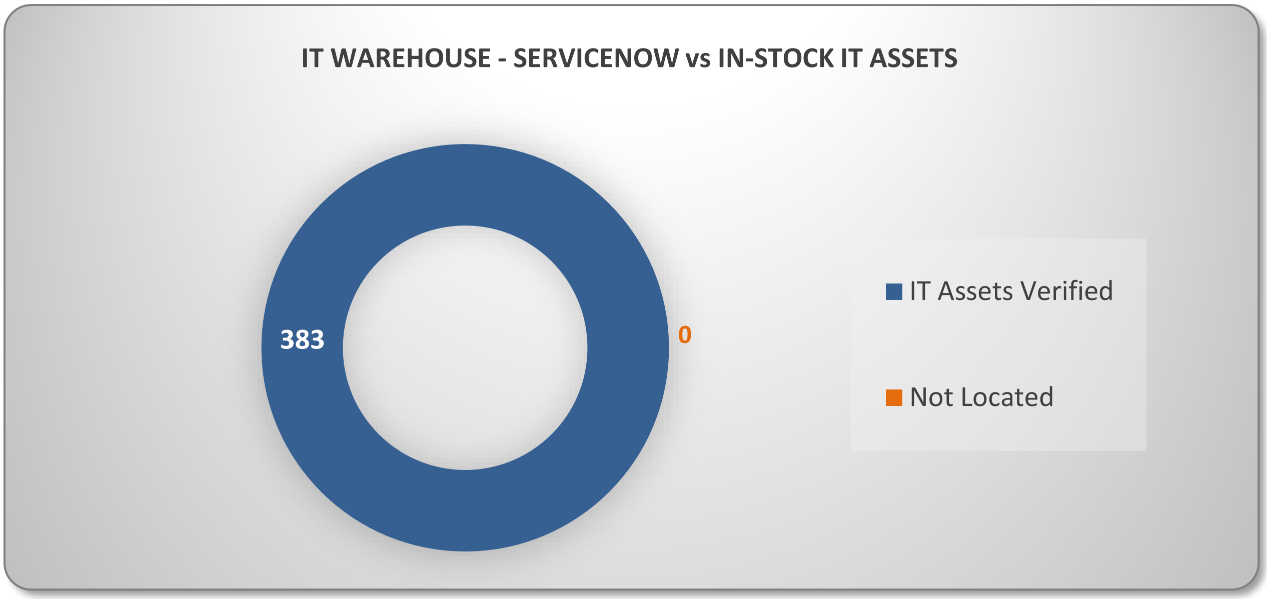
The Audit Team tested a total of 676 IT assets across eight (8) different county locations. Out of eight locations, 5 locations and 19 total assets (3%) contained discrepancies between the IT assets physically present and those recorded in ServiceNow. The results are categorized as follows:

- **Verified -** IT assets physically identified and matched to records in ServiceNow.
- **Not Located -** IT assets physically present but not located in the ServiceNow, or vice versa.



<u>Testing of In-Stock IT Assets</u>

On May 1, 2024, the Audit Team performed fieldwork testing at the IT warehouse located in 419 N Pierce St. A total of 383 assets were selected for testing. Of these, the Audit Team successfully identified 383 assets (100%).



RECOMMENDATION

To further enhance the accuracy and reliability of IT asset inventory records in ServiceNow, management should:

- Conduct a review of all locations listed in the system to identify and update outdated entries, such as Net Park.

- Implement asset management procedures to ensure all IT asset movements or disposals are accurately recorded in ServiceNow. This includes requiring mandatory updates to the system whenever assets are relocated or decommissioned. Providing training to applicable staff on these procedures is recommended to enhance their understanding of asset movement practices and ensure accountability for maintaining accurate records.

- Consider using ServiceNow's reporting and notification features to flag anomalies, such as assets listed at inactive locations or discrepancies between inventory data and physical counts.

CLIENT RESPONSE:

Concur

CORRECTIVE ACTION PLAN:

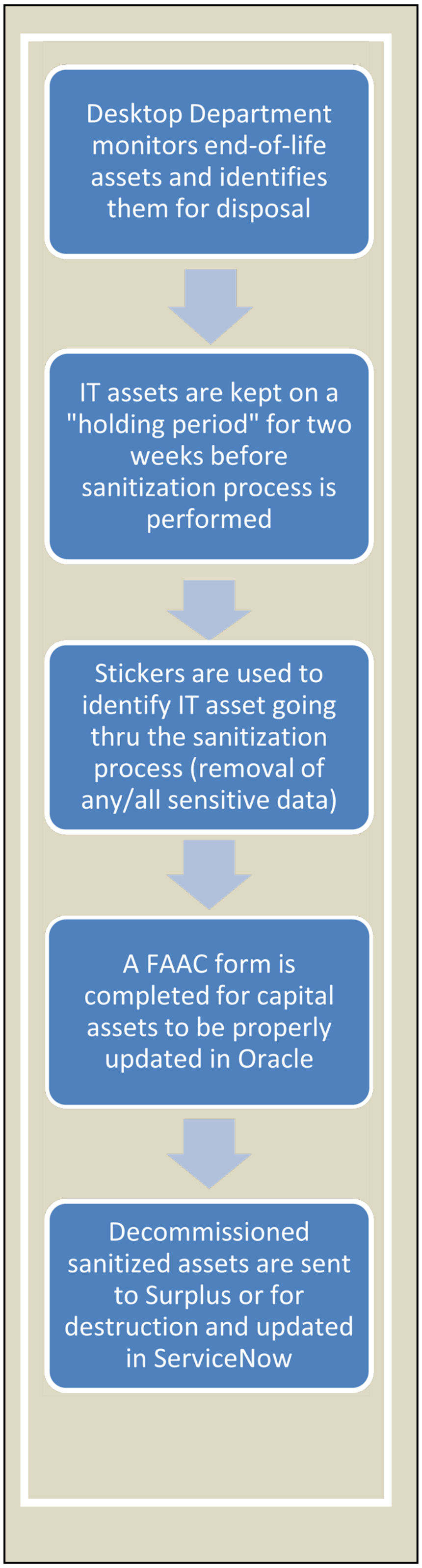
The Information & Innovation Office's portfolio of departments will develop a process and assess current workflows to ensure that locations and movements of assets and Configuration Items (CIs) are updated accurately. Appropriate training and reporting will be provided to the relevant stakeholders. The action plan includes:

- *Conduct a review of all locations listed in the system to identify and update outdated entries*
- *Implement asset management procedures to ensure all IT asset movements or disposals are accurately recorded in ServiceNow.*
- *Review current ServiceNow Hardware Asset Management (HAM) Processes and implement workflow automation for Procurement, Decommissioning, Stockroom transfers, etc.*
- *Review and document current GIS location integration and data model utilized in ServiceNow.*

TARGET COMPLETION DATE:

June 30, 2026

AUDIT COMMENT 3: ASSETS' END-OF-LIFE PROCESS



Desktop Department monitors end-of-life assets and identifies them for disposal

IT assets are kept on a "holding period" for two weeks before sanitization process is performed

Stickers are used to identify IT asset going thru the sanitization process (removal of any/all sensitive data)

A FAAC form is completed for capital assets to be properly updated in Oracle

Decommissioned sanitized assets are sent to Surplus or for destruction and updated in ServiceNow

Proper retirement and disposal procedures are followed by the ITD.

The objective was to determine whether or not end-of-life assets are retired in compliance with the Board decommissioning procedures. This includes verifying adherence to data sanitization protocols, obtaining required approvals, and ensuring accurate and proper recording of retired assets in system records.

<u>Background</u>

When IT assets or equipment reach the end of their useful life, the procedures for data removal and asset decommissioning vary depending on the asset's location and type (e.g., endpoint equipment vs. network or storage equipment). Work computers (personal PCs) typically have a lifecycle of five (5) years. The Desktop Department oversees these cycles, identifying computers due for replacement and preparing them for disposal.

In cases requiring immediate equipment replacement, the Desktop Team performs a "hot swap," creating an order in ServiceNow as a formal request for replacement from stock. For asset transfers and data sanitization, the Hardware Move Request form in ServiceNow is utilized.

Decommissioning of capitalized equipment requires confirmation from the IT Asset Management Department before being transferred to Surplus inventory, ensuring necessary general ledger (GL) entries are made by the Clerk's Office. A Fixed Assets Action Request (FAAC) form is used for this purpose.

When PCs or endpoint equipment are retired, the ServiceNow record is updated to reflect their new status and assigned to the "IT Infrastructure & Technical Support" team. A sanitization sticker is placed on the device, noting the date it was received, the recipient, and its status (Stock or Surplus). Within two weeks, the device undergoes data sanitization to securely remove all sensitive information. Devices that cannot be wiped are designated for hard drive destruction. Sanitized devices are then moved to the "Surplus rack" at the Surplus Warehouse.

Forms are emailed to the manager of the responsible team for approval. For Capital Assets, a memo is sent to the Clerk’s Capital Asset team for additional approvals. Once approved, the IT Asset Management team arranges for either the disposal or surplus of the equipment.

For surplus items, a record is created on either a Capital or Non-Capital Surplus form, and an appointment is scheduled with the Surplus Warehouse manager for drop-off. Items are transported to the Facilities’ Surplus Warehouse, where surplus forms are cross-verified and signed upon delivery. The ServiceNow record is then updated to reflect the new status as “Retired/Surplus”.

For items designated for destruction, a vendor is contacted and scheduled for equipment pick-up. Asset scanning and video documentation are completed and stored in the Hardware Asset Management network folder. The ServiceNow system is updated to reflect the destruction status and any relevant details.

TEST PROCEDURE

To evaluate the retirement and decommissioning processes for end-of-life IT assets, the Audit Team performed the following procedures:

1. Obtained a list of County-owned IT assets tracked in ServiceNow.
2. Collected IT surplus data records for April 2024 and compared them to ServiceNow data using unique Asset Tag Numbers as identifiers to identify any discrepancies.
3. Verified whether or not decommissioning procedures were properly followed by ensuring that:
    - Data sanitization methods were properly performed.
    - Transfer approvals were properly obtained.
    - Asset updates were accurately recorded in ServiceNow with a "Retired/Surplus" status.
    - Tested a random sample of ten (10) capital IT assets to ensure FAAC form data matched ServiceNow and Oracle records, including updated in surplus locations.

TESTING RESULTS

The Audit Team reviewed 197 IT assets sent to surplus in April 2024, comparing ServiceNow records with surplus data. Of these, 194 (98%) were correctly updated in ServiceNow as "Retired/Surplus." The following discrepancies were identified:

- Two (2) assets were not located in the ServiceNow data. These items were previously tagged but due to the change in the Procurement Policy, these are now treated as consumables.
- One (1) asset was not found in the initial ServiceNow records but was later verified through screenshots provided by the IT team.

All surplus assets reviewed had sanitization stickers documenting the date received, the responsible individual, and the sanitization or surplus status. No significant issues were noted regarding compliance with data sanitization protocols.

Additionally, based on the random sample of ten (10) capital IT assets tested by the Audit Team, the results showed that:

- Data recorded in the Fixed Assets Action Request (FAAC) forms matched ServiceNow and Oracle records for all but one (1) asset.
- One exception was identified where the serial number in Oracle did not match the serial number recorded in the FAAC form by one letter, which appeared to be a typographical error.

Other data points, such as asset tag numbers, location updates, and item descriptions, were consistent across all systems for the tested sample. All tested assets were appropriately retired and sent to surplus in compliance with decommissioning procedures.

RECOMMENDATION

The Audit Team did not identify any material concerns that required management's corrective actions.